Amendments to the Claims

The Claims have not been amended herein, but are included for the convenience of the Examiner.

1. (Previously Presented) A memory architecture, comprising:

   an unprotected memory space configured to store encrypted information, said encrypted information corresponding to a plain text version thereof, said unprotected memory space is located outside a microprocessor;

   a message digest corresponding to said encrypted information;

   a first protected memory space configured to store at least a subset of operating system instructions, said first protected memory space is located outside said microprocessor; and

   a second protected memory space configured to store said plain text version of said encrypted information, said second protected memory space is located outside said microprocessor;

wherein said operating system instructions in said first protected memory space operate on said plain text version of said encrypted information in said second protected memory space;

wherein a random access memory comprises said unprotected memory space, said first protected memory space, and said second protected memory space.

2. (Original) The memory architecture of Claim 1, wherein said encrypted information comprises an instruction to load said encrypted information from said unprotected memory space into said first protected memory space.

3. (Original) The memory architecture of Claim 2, further comprising one or more instructions to decrypt said encrypted information in said first protected memory space to form said plain text version.

4. (Original) The memory architecture of Claim 1, wherein said encrypted information comprises an instruction to store at least one of (i) said encrypted information in

said first protected memory space, (ii) said plain text version in said first protected memory space, and (iii) said plain text version in said second protected memory space.

5. (Original) The memory architecture of Claim 1, wherein said unprotected memory space is further configured to store executable code and data.

6. (Previously Presented) The memory architecture of Claim 1, wherein said subset of operating system instructions comprises at least one member selected from the group consisting of:
fetching or pre-fetching at least part of said executable code and data;
interpreting at least part of said executable code and data;
translating at least part of said executable code and data; and
determining whether information in said unprotected memory space comprises encrypted information.

7. (Original) The memory architecture of Claim 6, further comprising a third protected memory configured to store said plain text version after at least one operating system instruction has operated thereon.

8. (Previously Presented) The memory architecture of Claim 1, wherein said first protected memory space comprises said message digest.

9. (Previously Presented) The memory architecture of Claim 1, wherein said first protected memory space further comprises a table linking said message digest to said plain text version in said second protected memory space.

10. (Original) The memory architecture of Claim 9, wherein said table comprises a non-zero location of said plain text version in said second protected memory space.

11. (Previously Presented) The memory architecture of Claim 1, wherein said first protected memory space further comprises a table linking a unique identifier for said encrypted information to a pointer for at least one of (i) a location of said plain text version and (ii) a location of a decryption tool for decrypting said encrypted information.

12. (Previously Presented) A system for operating on encrypted information, comprising:

a microprocessor; and

a memory architecture of comprising:

an unprotected memory space configured to store encrypted information, said encrypted information corresponding to a plain text version thereof, said unprotected memory space is located outside said microprocessor;

a message digest corresponding to said encrypted information;

a first protected memory space configured to store at least a subset of operating system instructions, said first protected memory space is located outside said microprocessor; and

a second protected memory space configured to store said plain text version of said encrypted information, said second protected memory space is located outside said microprocessor, wherein said operating system instructions in said first protected memory space operate on said plain text version of said encrypted information in said second protected memory space;

wherein said microprocessor is configured to execute said operating system instructions;

wherein a hard drive comprises said unprotected memory space, said first protected memory space, and said second protected memory space.

13. (Previously Presented) The system of Claim 12, wherein said first protected memory space comprises a table.

14. (Previously Presented) The system of Claim 12, wherein said first protected memory space comprises said message digest.

15. (Previously Presented) The system of Claim 12, wherein said first protected memory space further comprises a table linking a unique identifier for said encrypted information to a pointer for a location of a decryption tool for decrypting said encrypted information.

16. (Original) The system of Claim 12, further comprising at least one peripheral device configured to operate in accordance with said encrypted information.

17. (Previously Presented) A method of operating on encrypted information, comprising:

transferring said encrypted information to a first protected memory address inaccessible to a user-accessible software program, but accessible to an operating system instruction set, said first protected memory address is located outside a microprocessor;

if said encrypted information comprises encrypted information, decrypting said encrypted information to form a decrypted version of said encrypted information, said decrypting comprises a message digest; and

storing said first protected memory address in a second protected memory address inaccessible to a user-accessible software program, but accessible to an operating system instruction set, wherein said second protected memory address is linked to an original location of said encrypted information, said second protected memory address is located outside said microprocessor;

wherein a detachable electronically erasable and programmable memory comprises said first protected memory address and said second protected memory address.

18. (Previously Presented) The method of Claim 17, wherein said encrypted information comprises encrypted information.

19. (Previously Presented) The method of Claim 18, wherein said original location of said encrypted information is in unprotected memory, wherein said detachable electronically erasable and programmable memory comprises said unprotected memory.

20. (Original) The method of Claim 18, further comprising linking a decryption key to at least one of said encrypted information, said original location and said first protected memory address.

21. (Previously Presented) The method of Claim 17, further comprising operating on said decrypted version information entirely within protected memory.

22. (Previously Presented) The method of Claim 21, wherein said protected memory comprises a table.

23. (Canceled)